

Sikringsrapport

Beskriver, hvad der blev sikret, hvordan og af hvem. Ingen analyse og ingen konklusion om sagen. Skriv rapporten samme dag som sikringen, ud fra noter og handlingslog. Afvigelser og fejl skal med. Grå rækker er fiktive eksempler, der kun viser formen.

1. Forside

Titel: Sikringsrapport, sag (navn eller nummer)

Dato for rapport

Udarbejdet af (navn, rolle, organisation)

Bestilt af (navn, rolle)

Version

2. Baggrund og formål

Kort og uden konklusioner. Skriv fx "der blev sikret en postkasse-eksport for perioden", ikke "medarbejderen sendte filer".

Hvorfor blev der sikret?

Hvilke spørgsmål skal sikringen kunne understøtte senere?

Hvem besluttede sikringen, og hvornår?

3. Kilder

Én linje pr. kilde. Brug samme bevis-id som i bevisloggen.

Bevis-id	Type (computer, server, telefon, postkasse, log, cloudkonto)	Identifikation (serienummer, hostnavn, konto, tenant)	Bruger eller ejer	Tilstand ved ankomst (tændt/slukket, låst, netværk, kryptering)
EKSEMPEL-E001	Eksempel: computer	Eksempel: SN-0000-FIKTIV	Eksempel: Medarbejder A	Eksempel: slukket, krypteret

4. Metode

Valgt sikringsmetode pr. kilde (image, logisk, målrettet, eksport, live) og begrundelse

Skrivebeskyttelse brugt

Værktøjer og versioner

Søgekriterier og tidsvinduer ved eksporter

Hvor beviskopierne blev gemt

5. Forløb

Kort tidslinje med klokkeslæt og tidszone: ankomst eller start, hændelser før sikringen (fx isolering fra netværk, nedlukning), start og slut for hver sikring, hashkontrol, forsegling og afslutning.

Dato og tid (tidszone)	Hændelse	Udført af	Bemærkning
2026-01-01 10:00 (UTC+1)	Eksempel: start af image af EKSEMPEL-E001	Eksempel: Tekniker B	

6. Resultat

Liste over beviskopier med bevis-id og hashværdi, eller henvisning til hash-log (bilag).

Bevis-id	Bevis kopi (filnavn eller objekt)	Algoritme	Hashværdi
EKSEMPEL-E002	EKSEMPEL-E002.E01	SHA-256	(64 hexadecimale tegn)

Hvad blev ikke sikret, og hvorfor (fx manglende nøgle, licens, utilgængelig enhed)

7. Afvigelser og indgreb

Ændringer på kilden før eller under sikringen (logins, genstarter, oprydning)

Fejl under sikringen og håndtering

Personer, der har haft adgang til kilden før sikringen

Det er afgørende for den senere analyse at kunne skille egne spor fra sagens. Henvis til handlingsloggen, hvis den findes.

8. Opbevaring

Opbevaringssted og adgangskontrol

Kryptering

Ansvarlig for opbevaring

9. Bilag

- ☐ Bevislog
- ☐ Hash-log
- ☐ Fotos
- ☐ Værktøjslogs
- ☐ Handlingslog (hvis ført)

10. Underskrift

Navn

Dato

Underskrift